REMARKS

The Office Action dated June 17, 2005, has been carefully reviewed and the foregoing amendment has been made in response thereto. Claims 1-31 are pending in the application.

The rejection of claims 1-8 under 35 USC 112, second paragraph, is respectfully traversed. The recitation of "audit records" has been deleted from claims 1 and 9. The claims now refer to log records relating to the use and attempted use of a respective member. Therefore, the claims are now definite and are in conformance with 35 USC 112.

The rejection of claims 1-31 under 35 USC 103(a) as being unpatentable over Hayes in view of Ko et al is respectfully traversed.

Regarding independent claims 1 and 9, the claimed invention includes a log server, a detection server, and a profile server operable to store an alert status indicative of identification of the occurrence of the threat condition by the detection server, wherein each of the plurality of members is operable to query the profile server in order to check an alert status, and, in response to an alert, to implement a pre-defined action. The claimed structure allows the present invention to provide a cooperative response of the domain to an attack while minimizing the overhead used by each of the members of the domain for performing security functions.

Hayes discloses that log information collected onto a collection server is analyzed by an expert system which looks for trends or known patterns that could indicate a problem with the network. In response to such trends, the network administrator can then take appropriate actions (col. 5, lines 34-42). Hayes lacks any teaching or suggestion of a profile server or any other ability of domain members to automatically respond to a threat.

Ko et al is cited for supposedly showing a profile server, but the reference fails to teach or suggest what is actually claimed. Ko et al teaches a multi-level security system for a computer network. Global and local analyzers communicate with *sensors* implemented in local computers. The sensor monitors activity in an assigned

portion of a network and can be constructed of a host-based intrusion detection system, a network sniffer, a firewall, etc. (column 5, lines 39-54). Thus, the sensors are a specialized unit performing security functions for themselves and other computers in a local area as opposed to the end device of the present invention which creates log records but has no threat detection capability itself that must send a query to a profile server to determine an alert status.

Contrary to the assertions in the rejection, Ko et al has no teaching or suggestion of "querying of the global analyzer by means of continuous attention to said server for any new condition that may require action." This characterization of Ko et al by the Office Action is not supported anywhere in the reference and it is contrary to the clear teachings whereby responses are communicated by the global analyzer to the local analyzers and from the local analyzers to the local sensors. By providing an agent within each domain member which initiates a periodic query to determine the presence of an alert, the present invention avoids the added computing resources and manual configuration efforts at both the server and the member devices that would be needed in order to push alert messages to the member end devices.

Claims 1 and 9 recite a profile server. Alert status is retrieved by the domain members by querying the profile server. Ko et al fails to teach or suggest any aspect of the global analyzer, the local analyzer, or the sensors wherein an alert status is stored in a server that can be queried by another device connected in the network. Thus, the combination of Hayes and Ko et al fails to produce the claimed elements of claims 1 and 9.

Besides failing to teach the recited elements, the rejection fails to demonstrate motivation for combining the references. Ko et al shows threat detection taking place at all levels of its system, even in the local sensors. Furthermore, there is no teaching of log files in Ko et al. Therefore, there would be no reason to modify Hayes in view of Ko et al.

In view of the foregoing, claims 1 and 9 and their dependent claims 2-8 and 10-15 are allowable.

Claims 5 and 13 are additionally patentable for the reason that the security

profile stored by the profile server includes elements completely lacking from the cited references. Since neither Hayes nor Ko et al teaches any querying initiated by the domain members, there is likewise no teaching or suggestion of a security profile having configurable values for the updating frequency of the alert queries or configuration refresh queries for updating the security profile.

Claims 7 and 9 are additionally patentable for the reason that there is no teaching or suggestion in the cited references of the use of a non-routable protocol for broadcasting a message to communicate occurrence of a threat condition to an edge device. A non-routable protocol cannot pass through a router and can only be sent between devices by a fixed route. The cited passages in Ko et al refer to communications through a wide area network. It is known in the art that a wide area network requires a routable protocol. Furthermore, other portions of Ko et al dealing with communications within the local network portions fail to teach or suggest any use of a non-routable protocol or any reasons why such a protocol could be desirable.

Independent claims 16 and 24 recite limitations similar to claims 1 and 9 and are allowable for the same reasons together with their dependent claims.

In view of the foregoing amendment and remarks, claims 1-31 are now in condition for allowance. Favorable action is respectfully solicited.

Respectfully submitted,

Mark L. Mollon
Attorney for Applicant(s)
Reg. No. 31,123

Dated: August 9, 2005
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fourth Floor
720 Water Street
Toledo, Ohio 43604
(734) 542-0900
(734) 542-9569 (fax)